



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|-------------|----------------------|-----------------------|------------------|
| 09/836,214 | 04/18/2001 | Peter T. Dinsmore | NAIIP089/00.175.01 | 6427 |
| 28875 | 7590 | 11/24/2004 | EXAMINER | |
| Zilka-Kotab, PC P.O. BOX 721120 SAN JOSE, CA 95172-1120 | | | LAFORGIA, CHRISTIAN A | |
| | | | ART UNIT | PAPER NUMBER |
| | | | 2131 | |

DATE MAILED: 11/24/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

| | | | |
|------------------------------|------------------------|---------------------|--|
| Office Action Summary | Application No. | Applicant(s) | |
| | 09/836,214 | DINSMORE ET AL. | |
| | Examiner | Art Unit | |
| | Christian La Forgia | 2131 | |

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 02 July 2002.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-25 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-25 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 18 April 2001 is/are: a) ☐ accepted or b) ☒ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date <u>9/7/01; 6/19/02</u> | 6) <input type="checkbox"/> Other: _____ |

Art Unit: 2131

DETAILED ACTION

1. Claims 1-25 have been presented for examination.

Specification

2. The following guidelines illustrate the preferred layout for the specification of a utility application. These guidelines are suggested for the applicant's use.

Arrangement of the Specification

As provided in 37 CFR 1.77(b), the specification of a utility application should include the following sections in order. Each of the lettered items should appear in upper case, without underlining or bold type, as a section heading. If no text follows the section heading, the phrase "Not Applicable" should follow the section heading:

- (a) TITLE OF THE INVENTION.
- (b) CROSS-REFERENCE TO RELATED APPLICATIONS.
- (c) STATEMENT REGARDING FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT.
- (d) INCORPORATION-BY-REFERENCE OF MATERIAL SUBMITTED ON A COMPACT DISC (See 37 CFR 1.52(e)(5) and MPEP 608.05. Computer program listings (37 CFR 1.96(c)), "Sequence Listings" (37 CFR 1.821(c)), and tables having more than 50 pages of text are permitted to be submitted on compact discs.) or
REFERENCE TO A "MICROFICHE APPENDIX" (See MPEP § 608.05(a). "Microfiche Appendices" were accepted by the Office until March 1, 2001.)
- (e) BACKGROUND OF THE INVENTION.
 - (1) Field of the Invention.
 - (2) Description of Related Art including information disclosed under 37 CFR 1.97 and 1.98.
- (f) BRIEF SUMMARY OF THE INVENTION.
- (g) BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWING(S).
- (h) DETAILED DESCRIPTION OF THE INVENTION.
- (i) CLAIM OR CLAIMS (commencing on a separate sheet).
- (j) ABSTRACT OF THE DISCLOSURE (commencing on a separate sheet).
- (k) SEQUENCE LISTING (See MPEP § 2424 and 37 CFR 1.821-1.825. A "Sequence Listing" is required on paper if the application discloses a nucleotide or amino acid sequence as defined in 37 CFR 1.821(a) and if the required "Sequence Listing" is not submitted as an electronic document on compact disc).

The instant application is missing the section "Brief Summary of the Invention." Appropriate action is required.

Art Unit: 2131

Drawings

3. Figures 1 and 2 should be designated by a legend such as --Prior Art-- because only that which is old is illustrated. See MPEP § 608.02(g). Corrected drawings in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. The replacement sheet(s) should be labeled "Replacement Sheet" in the page header (as per 37 CFR 1.121(d)) so as not to obstruct any portion of the drawing figures. If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. The variable "D" in "D-ary" in claims 10 and 23 is a relative term which renders the claim indefinite. The variable "D" in "D-ary" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Art Unit: 2131

7. Claims 1, 3, 11-14, 17, 24, and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Ioulus: A Framework for Scalable Secure Multicasting*, by Suvo Mittra, hereinafter Mittra, in view of U.S. Patent No. 6,606,706 B1 to Li, hereinafter Li.
8. As per claims 1, 11, 17, 24, and 25, Mittra discloses associating a subgroup of a group with a leaf node of a hierarchical tree (p. 280, column 2, i.e. “The secure distribution tree is composed of a number of smaller secure multicast “subgroups” arranged in a hierarchy to create a single virtual secure multicast group,” wherein the leaf node is drawn to the “group security intermediaries” or “group security agents”).
9. Mittra also discloses wherein the leaf node has a leaf key common to the members of the subgroup (p. 280, column 2, i.e. “Moreover, each group has its own subgroup keying material (K_{SGRP} in short) and there is no global K_{GRP} .”)
10. Mittra discusses two types of evictions of members from the groups (p. 282, column 2, i.e. “(1) a member wishes to voluntarily leave the subgroup in which case it sends a LEAVE request to the GSA, or (2) the GSA wants to expel a member of the subgroup and sends a notification to that effect to the expelled member”).
11. Mittra does not disclose wherein leaf key enables the members of the subgroup to receive an update message for an interior node above the leaf node.
12. It would have been obvious to one of ordinary skill in the art at the time the invention was made to have the leaf key enable members of the subgroup to receive an update message from an interior node that is above the leaf node (Li, column 10, lines 5-14, column 11, lines 34-43), since Li states at column 2, lines 12-25 that such a modification would reduce latency incurred by decrypting and re-encrypting data received from and transmitted to each subgroup.

Art Unit: 2131

13. Regarding claim 3, Mittra discloses wherein said evicted member is part of said subgroup (p. 282-283, **Section 6.4 Leaves**).

14. Regarding claim 12, Mittra discloses wherein said evicting comprises evicting one member of said group (p. 282-283, **Section 6.4 Leaves**).

15. Regarding claim 13, Mittra teaches wherein said evicting comprises evicting more than one member of said group (p. 282-283, **Section 6.4 Leaves**).

16. Regarding claim 14, Mittra discloses wherein said notifying comprises transmitting identities of said at least one evicted member (p. 282-283, **Section 6.4 Leaves**).

17. Claim 2 is rejected under 35 U.S.C. 103(a) as being unpatentable over Mittra and Li as applied to claim 1 above, and further in view of **Dynamic Cryptographic Context Managemnt**, by David M. Balenson et al., hereinafter Balenson.

18. Regarding claim 2, Mittra and Li do not disclose wherein said evicted member is not a part of said subgroup.

19. It would have been obvious to one of ordinary skill in the art at the time the invention was made to re-key if the evicted member was not part of the subgroup, since Balenson states on page 8 that such a modification would prevent the evictee from knowing the keys associated with tree.

20. Claims 4, 5, 9, 10, 15, 16, 18, 22, and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mittra and Li as applied above, and further in view of U.S. Patent No. 6,240,188 to Dondeti et al., hereinafter Dondeti.

21. With regards to claims 4 and 15, Mittra and Li do not teach wherein said subgroup is a self-repairing group, said self-repairing group being operative to update said leaf key independently.

22. It would have been obvious to one of ordinary skill in the art at the time the invention was made to make the subgroup a self-repairing group, being operative to update the leaf key independently, since Dondeti states at column 2, lines 19-53 that such a modification would make key distribution scalable to larger numbers of users, as it would reduce the flooding of control traffic.

23. Concerning claims 5, 16, and 18, Dondeti teaches wherein said self-repairing group uses a reusable power set (column 3, lines 47-63).

24. Regarding claims 9 and 22, Mittra and Li do not disclose wherein said hierarchical tree is a binary tree.

25. It would have been obvious to one of ordinary skill in the art at the time the invention was made for the hierarchical tree to be a binary tree, since Dondeti discloses the need for balancing the key tree at column 10, lines 29-39

Art Unit: 2131

26. Regarding claims 10 and 23, Mittra and Li do not disclose wherein said hierarchical tree is a D-ary tree.

27. It would have been obvious to one of ordinary skill in the art at the time the invention was made for the hierarchical tree to be a D-ary tree, since Dondeti discloses the need for balancing the key tree at column 10, lines 29-39, wherein the D-ary tree is a binary tree.

28. Claims 6-8 and 19-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mittra and Li as applied to claim 1 above, and further in view of **Key Management for Large Dynamic Groups: One-Way Function Trees and Amortized Initialization**, by D. McGrew et al., hereinafter McGrew.

29. Regarding claims 6 and 19, Mittra and Li do not disclose wherein key updates are performed using a logical key hierarchy method.

30. It would have been obvious to one of ordinary skill in the art at the time the invention was made to use a logical key hierarchy method, since McGrew discloses on page 21 that such a modification would use trusted routers, thereby creating an added security measure.

31. Regarding claims 7 and 20, Mittra and Li do not disclose wherein key updates are performed using a one-way function tree method.

32. It would have been obvious to one of ordinary skill in the art at the time the invention was made to use a one-way function tree method, since McGrew discloses on page 9 that using a one-way tree function has provable security properties.

Art Unit: 2131

33. Regarding claims 8 and 21, Mittra and Li do not teach wherein key updates are performed using a one-way function chain method.

34. It would have been obvious to one of ordinary skill in the art at the time the invention was made to use a one-way function chain method, since McGrew discloses on page 9 that using a one-way tree function has provable security properties.

Double Patenting

35. A rejection based on double patenting of the "same invention" type finds its support in the language of 35 U.S.C. 101 which states that "whoever invents or discovers any new and useful process ... may obtain a patent therefor ..." (Emphasis added). Thus, the term "same invention," in this context, means an invention drawn to identical subject matter. See *Miller v. Eagle Mfg. Co.*, 151 U.S. 186 (1894); *In re Ockert*, 245 F.2d 467, 114 USPQ 330 (CCPA 1957); and *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970).

36. A statutory type (35 U.S.C. 101) double patenting rejection can be overcome by canceling or amending the conflicting claims so they are no longer coextensive in scope. The filing of a terminal disclaimer cannot overcome a double patenting rejection based upon 35 U.S.C. 101.

37. Claims 1-25 are provisionally rejected under 35 U.S.C. 101 as claiming the same invention as that of claims 1-25 of copending Application No. 09/836,238. This is a provisional double patenting rejection since the conflicting claims have not in fact been patented.

Conclusion

38. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Art Unit: 2131

39. The following patents are cited to further show the state of the art with respect to re-keying in multicasting environments, such as:

United States Patent No. 6,226,743 to Naor et al., which is cited to show an authenticated search tree that serves for authenticating membership.

United States Patent No. 6,397,329 to Aiello et al., which is cited to show a certificate revocation scheme that uses a binary tree structure.

United States Patent No. 5,592,552 to Fiat, which is cited to show selective broadcasting to a plurality of subscriber subsets within a set of subscribers.

United States Patent No. 6,584,566 to Hardjono, which is cited to show distributed group key management for multicast security.

United States Patent No. 5,748,736 to Mittra, which is cited to show secure group communication via multicast.

United States Patent No. 6,295,361 to Kadansky et al., which is cited to show changing a group key for all nodes in a multicasting group.

40. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian La Forgia whose telephone number is (571) 272-3792. The examiner can normally be reached on Monday thru Thursday 7-5.

41. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Art Unit: 2131

42. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Christian LaForgia
Patent Examiner
Art Unit 2131

clf


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100